Exam II Review

Shaoyun Yi

MATH 546/701I

University of South Carolina

June 8, 2020

Review

- A group isomorphism $\phi : (G_1, *) \xrightarrow{\cong} (G_2, \cdot)$

Review

- A group isomorphism $\phi : (G_1, *) \xrightarrow{\cong} (G_2, \cdot)$
  - Find ϕ & Verify ϕ

Review

- A group isomorphism $\phi : (G_1, *) \xrightarrow{\cong} (G_2, \cdot)$
  - Find ϕ & Verify ϕ
  - $\phi(a^n) = (\phi(a))^n$ for all $a \in G_1$ and all $n \in \mathbf{Z}$: $n = 0$ vs. $n = -1$

Review

- A group isomorphism $\phi : (G_1, *) \xrightarrow{\cong} (G_2, \cdot)$
  - Find ϕ & Verify ϕ
  - $\phi(a^n) = (\phi(a))^n$ for all $a \in G_1$ and all $n \in \mathbf{Z}$: $n = 0$ vs. $n = -1$
  - $o(a) = n \Rightarrow o(\phi(a)) = n$; abelian; cyclic
- Lagrange's Theorem:

Review

- A group isomorphism $\phi : (G_1, *) \xrightarrow{\cong} (G_2, \cdot)$
  - Find ϕ & Verify ϕ
  - $\phi(a^n) = (\phi(a))^n$ for all $a \in G_1$ and all $n \in \mathbf{Z}$: $n = 0$ vs. $n = -1$
  - $o(a) = n \Rightarrow o(\phi(a)) = n$; abelian; cyclic
- Lagrange's Theorem: If $|G| = n < \infty$ and $H \subseteq G$, then $|H| \big| n$.

Review

- A group isomorphism $\phi : (G_1, *) \xrightarrow{\cong} (G_2, \cdot)$
  - Find ϕ & Verify ϕ
  - $\phi(a^n) = (\phi(a))^n$ for all $a \in G_1$ and all $n \in \mathbf{Z}$: $n = 0$ vs. $n = -1$
  - $o(a) = n \Rightarrow o(\phi(a)) = n$; abelian; cyclic
- Lagrange's Theorem: If $|G| = n < \infty$ and $H \subseteq G$, then $|H| \big| n$.
  - Let $a \in G$. Then $\langle a \rangle \subseteq G$ and $|\langle a \rangle| = o(a) \big| |G|$ in addition if G is finite.

Review

- A group isomorphism $\phi : (G_1, *) \xrightarrow{\cong} (G_2, \cdot)$
  - Find ϕ & Verify ϕ
  - $\phi(a^n) = (\phi(a))^n$ for all $a \in G_1$ and all $n \in \mathbf{Z}$: $n = 0$ vs. $n = -1$
  - $o(a) = n \Rightarrow o(\phi(a)) = n$; abelian; cyclic
- Lagrange's Theorem: If $|G| = n < \infty$ and $H \subseteq G$, then $|H| \big| n$.
  - Let $a \in G$. Then $\langle a \rangle \subseteq G$ and $|\langle a \rangle| = o(a) \big| |G|$ in addition if G is finite.
  - Any group of prime order is cyclic (and so abelian).
- Cayley's Theorem:

Review

- A group isomorphism $\phi : (G_1, *) \xrightarrow{\cong} (G_2, \cdot)$
  - Find ϕ & Verify ϕ
  - $\phi(a^n) = (\phi(a))^n$ for all $a \in G_1$ and all $n \in \mathbf{Z}$: $n = 0$ vs. $n = -1$
  - $o(a) = n \Rightarrow o(\phi(a)) = n$; abelian; cyclic
- Lagrange's Theorem: If $|G| = n < \infty$ and $H \subseteq G$, then $|H| \big| n$.
  - Let $a \in G$. Then $\langle a \rangle \subseteq G$ and $|\langle a \rangle| = o(a) \big| |G|$ in addition if G is finite.
  - Any group of prime order is cyclic (and so abelian).
- Cayley's Theorem: Every group is isomorphic to a permutation group.
- *Cyclic group* C_n:

Review

- A group isomorphism $\phi : (G_1, *) \xrightarrow{\cong} (G_2, \cdot)$
  - Find ϕ & Verify ϕ
  - $\phi(a^n) = (\phi(a))^n$ for all $a \in G_1$ and all $n \in \mathbf{Z}$: $n = 0$ vs. $n = -1$
  - $o(a) = n \Rightarrow o(\phi(a)) = n$; abelian; cyclic
- Lagrange's Theorem: If $|G| = n < \infty$ and $H \subseteq G$, then $|H| \big| n$.
  - Let $a \in G$. Then $\langle a \rangle \subseteq G$ and $|\langle a \rangle| = o(a) \big| |G|$ in addition if G is finite.
  - Any group of prime order is cyclic (and so abelian).
- Cayley's Theorem: Every group is isomorphic to a permutation group.
- *Cyclic group* C_n: Infinite: $\cong \mathbf{Z}$ vs. Finite: $\cong \mathbf{Z}_n \dashrightarrow$ multiplicative G

Review

- A group isomorphism $\phi : (G_1, *) \xrightarrow{\cong} (G_2, \cdot)$
  - Find ϕ & Verify ϕ
  - $\phi(a^n) = (\phi(a))^n$ for all $a \in G_1$ and all $n \in \mathbf{Z}$: $n = 0$ vs. $n = -1$
  - $o(a) = n \Rightarrow o(\phi(a)) = n$; abelian; cyclic
- Lagrange's Theorem: If $|G| = n < \infty$ and $H \subseteq G$, then $|H| \mid n$.
  - Let $a \in G$. Then $\langle a \rangle \subseteq G$ and $|\langle a \rangle| = o(a) \mid |G|$ in addition if G is finite.
  - Any group of prime order is cyclic (and so abelian).
- Cayley's Theorem: Every group is isomorphic to a permutation group.
- *Cyclic group* C_n: Infinite: $\cong \mathbf{Z}$ vs. Finite: $\cong \mathbf{Z}_n \dashrightarrow$ multiplicative G

  Subgroups of $\mathbf{Z}$ vs. Subgroups of $\mathbf{Z}_n \rightsquigarrow$ *subgroup diagram*
- *Dihedral group* D_n:

Review

- A group isomorphism $\phi : (G_1, *) \xrightarrow{\cong} (G_2, \cdot)$
  - Find ϕ & Verify ϕ
  - $\phi(a^n) = (\phi(a))^n$ for all $a \in G_1$ and all $n \in \mathbf{Z}$: $n = 0$ vs. $n = -1$
  - $o(a) = n \Rightarrow o(\phi(a)) = n$; abelian; cyclic
- Lagrange's Theorem: If $|G| = n < \infty$ and $H \subseteq G$, then $|H| \big| n$.
  - Let $a \in G$. Then $\langle a \rangle \subseteq G$ and $|\langle a \rangle| = o(a) \big| |G|$ in addition if G is finite.
  - Any group of prime order is cyclic (and so abelian).
- Cayley's Theorem: Every group is isomorphic to a permutation group.
- *Cyclic group* C_n: Infinite: $\cong \mathbf{Z}$ vs. Finite: $\cong \mathbf{Z}_n \dashrightarrow$ multiplicative G
  Subgroups of $\mathbf{Z}$ vs. Subgroups of $\mathbf{Z}_n \rightsquigarrow$ *subgroup diagram*
- *Dihedral group* D_n: Subgroups of D_3, D_4
- *Alternating group* A_n:

Review

- A group isomorphism $\phi : (G_1, *) \xrightarrow{\cong} (G_2, \cdot)$
  - Find ϕ & Verify ϕ
  - $\phi(a^n) = (\phi(a))^n$ for all $a \in G_1$ and all $n \in \mathbf{Z}$: $n = 0$ vs. $n = -1$
  - $o(a) = n \Rightarrow o(\phi(a)) = n$; abelian; cyclic
- Lagrange's Theorem: If $|G| = n < \infty$ and $H \subseteq G$, then $|H| \big| n$.
  - Let $a \in G$. Then $\langle a \rangle \subseteq G$ and $|\langle a \rangle| = o(a) \big| |G|$ in addition if G is finite.
  - Any group of prime order is cyclic (and so abelian).
- Cayley's Theorem: Every group is isomorphic to a permutation group.
- *Cyclic group* C_n: Infinite: $\cong \mathbf{Z}$ vs. Finite: $\cong \mathbf{Z}_n \dashrightarrow$ multiplicative G
  Subgroups of $\mathbf{Z}$ vs. Subgroups of $\mathbf{Z}_n \rightsquigarrow$ *subgroup diagram*
- *Dihedral group* D_n: Subgroups of D_3, D_4
- *Alternating group* A_n: Subgroups of A_3, A_4

Review

- A group isomorphism $\phi : (G_1, *) \xrightarrow{\cong} (G_2, \cdot)$
  - Find ϕ & Verify ϕ
  - $\phi(a^n) = (\phi(a))^n$ for all $a \in G_1$ and all $n \in \mathbf{Z}$: $n = 0$ vs. $n = -1$
  - $o(a) = n \Rightarrow o(\phi(a)) = n$; abelian; cyclic
- Lagrange's Theorem: If $|G| = n < \infty$ and $H \subseteq G$, then $|H| \,\big|\, n$.
  - Let $a \in G$. Then $\langle a \rangle \subseteq G$ and $|\langle a \rangle| = o(a) \,\big|\, |G|$ in addition if G is finite.
  - Any group of prime order is cyclic (and so abelian).
- Cayley's Theorem: Every group is isomorphic to a permutation group.
- *Cyclic group* C_n: Infinite: $\cong \mathbf{Z}$ vs. Finite: $\cong \mathbf{Z}_n \dashrightarrow$ multiplicative G

  Subgroups of $\mathbf{Z}$ vs. Subgroups of $\mathbf{Z}_n \rightsquigarrow$ *subgroup diagram*
- *Dihedral group* D_n: Subgroups of D_3, D_4
- *Alternating group* A_n: Subgroups of A_3, A_4
- $\mathbf{Z}_n^\times$: *not* always cyclic.

Review

- A group isomorphism $\phi : (G_1, *) \xrightarrow{\cong} (G_2, \cdot)$
  - Find ϕ & Verify ϕ
  - $\phi(a^n) = (\phi(a))^n$ for all $a \in G_1$ and all $n \in \mathbf{Z}$: $n = 0$ vs. $n = -1$
  - $o(a) = n \Rightarrow o(\phi(a)) = n$; abelian; cyclic
- Lagrange's Theorem: If $|G| = n < \infty$ and $H \subseteq G$, then $|H| \big| n$.
  - Let $a \in G$. Then $\langle a \rangle \subseteq G$ and $|\langle a \rangle| = o(a) \big| |G|$ in addition if G is finite.
  - Any group of prime order is cyclic (and so abelian).
- Cayley's Theorem: Every group is isomorphic to a permutation group.
- *Cyclic group* C_n: Infinite: $\cong \mathbf{Z}$ vs. Finite: $\cong \mathbf{Z}_n \dashrightarrow$ multiplicative G

  Subgroups of $\mathbf{Z}$ vs. Subgroups of $\mathbf{Z}_n \rightsquigarrow$ *subgroup diagram*
- *Dihedral group* D_n: Subgroups of D_3, D_4
- *Alternating group* A_n: Subgroups of A_3, A_4
- $\mathbf{Z}_n^\times$: *not* always cyclic. $|\mathbf{Z}_n^\times| = \varphi(n) = \#$ of generators of $\mathbf{Z}_n$

Review

- A group isomorphism $\phi : (G_1, *) \xrightarrow{\cong} (G_2, \cdot)$
  - Find ϕ & Verify ϕ
  - $\phi(a^n) = (\phi(a))^n$ for all $a \in G_1$ and all $n \in \mathbf{Z}$: $n = 0$ vs. $n = -1$
  - $o(a) = n \Rightarrow o(\phi(a)) = n$; abelian; cyclic
- Lagrange's Theorem: If $|G| = n < \infty$ and $H \subseteq G$, then $|H| \big| n$.
  - Let $a \in G$. Then $\langle a \rangle \subseteq G$ and $|\langle a \rangle| = o(a) \big| |G|$ in addition if G is finite.
  - Any group of prime order is cyclic (and so abelian).
- Cayley's Theorem: Every group is isomorphic to a permutation group.
- *Cyclic group* C_n: Infinite: $\cong \mathbf{Z}$ vs. Finite: $\cong \mathbf{Z}_n \dashrightarrow$ multiplicative G
  Subgroups of $\mathbf{Z}$ vs. Subgroups of $\mathbf{Z}_n \rightsquigarrow$ *subgroup diagram*
- *Dihedral group* D_n: Subgroups of D_3, D_4
- *Alternating group* A_n: Subgroups of A_3, A_4
- $\mathbf{Z}_n^\times$: *not* always cyclic. $|\mathbf{Z}_n^\times| = \varphi(n) = \#$ of generators of $\mathbf{Z}_n$
- Product of two subgroups: *not* always a subgroup.

Review

- A group isomorphism $\phi : (G_1, *) \xrightarrow{\cong} (G_2, \cdot)$
  - Find ϕ & Verify ϕ
  - $\phi(a^n) = (\phi(a))^n$ for all $a \in G_1$ and all $n \in \mathbf{Z}$: $n = 0$ vs. $n = -1$
  - $o(a) = n \Rightarrow o(\phi(a)) = n$; abelian; cyclic
- Lagrange's Theorem: If $|G| = n < \infty$ and $H \subseteq G$, then $|H| \big| n$.
  - Let $a \in G$. Then $\langle a \rangle \subseteq G$ and $|\langle a \rangle| = o(a) \big| |G|$ in addition if G is finite.
  - Any group of prime order is cyclic (and so abelian).
- Cayley's Theorem: Every group is isomorphic to a permutation group.
- *Cyclic group* C_n: Infinite: $\cong \mathbf{Z}$ vs. Finite: $\cong \mathbf{Z}_n \dashrightarrow$ multiplicative G
  Subgroups of $\mathbf{Z}$ vs. Subgroups of $\mathbf{Z}_n \rightsquigarrow$ *subgroup diagram*
- *Dihedral group* D_n: Subgroups of D_3, D_4
- *Alternating group* A_n: Subgroups of A_3, A_4
- $\mathbf{Z}_n^\times$: *not* always cyclic. $|\mathbf{Z}_n^\times| = \varphi(n) = \#$ of generators of $\mathbf{Z}_n$
- Product of two subgroups: *not* always a subgroup.
- Direct product of 2 groups $\rightsquigarrow$ n groups: $\mathbf{Z}_n \cong \mathbf{Z}_{p_1^{\alpha_1}} \times \cdots \mathbf{Z}_{p_m^{\alpha_m}} \rightsquigarrow \varphi(n)$

Example 1

Let G be an abelian group with subgroups H and K. Prove that if $HK = G$ and $H \cap K = \{e\}$, then $G \cong H \times K$.

Proof.

Example 1

Let G be an abelian group with subgroups H and K. Prove that if $HK = G$ and $H \cap K = \{e\}$, then $G \cong H \times K$.

Proof.

Define $\phi : H \times K \to G$ by $\phi((h, k)) = hk$, for all $(h, k) \in H \times K$.

(i) well-defined:

Example 1

Let G be an abelian group with subgroups H and K. Prove that if $HK = G$ and $H \cap K = \{e\}$, then $G \cong H \times K$.

Proof.

Define $\phi : H \times K \to G$ by $\phi((h,k)) = hk$, for all $(h,k) \in H \times K$.

(i) well-defined: Trivial. (Why?)

(ii) ϕ preserves the products:

Example 1

Let G be an abelian group with subgroups H and K. Prove that if $HK = G$ and $H \cap K = \{e\}$, then $G \cong H \times K$.

Proof.

Define $\phi : H \times K \to G$ by $\phi((h,k)) = hk$, for all $(h,k) \in H \times K$.

(i) well-defined: Trivial. (Why?)

(ii) ϕ preserves the products: For all $(h_1, k_1), (h_2, k_2) \in H \times K$ we have

$$\begin{aligned}\phi((h_1,k_1)(h_2,k_2)) &= \phi((h_1 h_2, k_1 k_2)) \\ &= h_1 h_2 k_1 k_2 \overset{!}{=} h_1 k_1 h_2 k_2 \\ &= \phi((h_1,k_1))\phi((h_2,k_2))\end{aligned}$$

(iii) one-to-one:

Example 1

Let G be an abelian group with subgroups H and K. Prove that if $HK = G$ and $H \cap K = \{e\}$, then $G \cong H \times K$.

Proof.

Define $\phi : H \times K \to G$ by $\phi((h, k)) = hk$, for all $(h, k) \in H \times K$.

(i) well-defined: Trivial. (Why?)

(ii) ϕ preserves the products: For all $(h_1, k_1), (h_2, k_2) \in H \times K$ we have

$$\begin{aligned}\phi((h_1, k_1)(h_2, k_2)) &= \phi((h_1 h_2, k_1 k_2)) \\ &= h_1 h_2 k_1 k_2 \overset{!}{=} h_1 k_1 h_2 k_2 \\ &= \phi((h_1, k_1))\phi((h_2, k_2))\end{aligned}$$

(iii) one-to-one: If $\phi((h, k)) = e$ for $(h, k) \in H \times K$, then we have $hk = e$.

$$hk = e \Rightarrow h = k^{-1} \in H \cap K \text{ (Why?)}$$

Example 1

Let G be an abelian group with subgroups H and K. Prove that if $HK = G$ and $H \cap K = \{e\}$, then $G \cong H \times K$.

Proof.

Define $\phi : H \times K \to G$ by $\phi((h,k)) = hk$, for all $(h,k) \in H \times K$.

(i) well-defined: Trivial. (Why?)

(ii) ϕ preserves the products: For all $(h_1,k_1),(h_2,k_2) \in H \times K$ we have

$$\begin{aligned}\phi((h_1,k_1)(h_2,k_2)) &= \phi((h_1h_2,k_1k_2)) \\ &= h_1h_2k_1k_2 \overset{!}{=} h_1k_1h_2k_2 \\ &= \phi((h_1,k_1))\phi((h_2,k_2))\end{aligned}$$

(iii) one-to-one: If $\phi((h,k)) = e$ for $(h,k) \in H \times K$, then we have $hk = e$.

$$hk = e \Rightarrow h = k^{-1} \in H \cap K \text{ (Why?)}$$

It follows that $h = k = e$. (Why?)

Example 1

Let G be an abelian group with subgroups H and K. Prove that if $HK = G$ and $H \cap K = \{e\}$, then $G \cong H \times K$.

Proof.

Define $\phi : H \times K \to G$ by $\phi((h, k)) = hk$, for all $(h, k) \in H \times K$.

(i) well-defined: Trivial. (Why?)

(ii) ϕ preserves the products: For all $(h_1, k_1), (h_2, k_2) \in H \times K$ we have

$$\begin{aligned}\phi((h_1, k_1)(h_2, k_2)) &= \phi((h_1 h_2, k_1 k_2)) \\ &= h_1 h_2 k_1 k_2 \overset{!}{=} h_1 k_1 h_2 k_2 \\ &= \phi((h_1, k_1))\phi((h_2, k_2))\end{aligned}$$

(iii) one-to-one: If $\phi((h, k)) = e$ for $(h, k) \in H \times K$, then we have $hk = e$.

$$hk = e \Rightarrow h = k^{-1} \in H \cap K \text{ (Why?)}$$

It follows that $h = k = e$. (Why?) Thus, ϕ is one-to-one. (Why?)

(iv) onto:

Example 1

Let G be an abelian group with subgroups H and K. Prove that if $HK = G$ and $H \cap K = \{e\}$, then $G \cong H \times K$.

Proof.

Define $\phi : H \times K \to G$ by $\phi((h, k)) = hk$, for all $(h, k) \in H \times K$.

(i) well-defined: Trivial. (Why?)

(ii) ϕ preserves the products: For all $(h_1, k_1), (h_2, k_2) \in H \times K$ we have

$$\begin{aligned} \phi((h_1, k_1)(h_2, k_2)) =& \phi((h_1 h_2, k_1 k_2)) \\ =& h_1 h_2 k_1 k_2 \stackrel{!}{=} h_1 k_1 h_2 k_2 \\ =& \phi((h_1, k_1))\phi((h_2, k_2)) \end{aligned}$$

(iii) one-to-one: If $\phi((h, k)) = e$ for $(h, k) \in H \times K$, then we have $hk = e$.

$$hk = e \Rightarrow h = k^{-1} \in H \cap K \text{ (Why?)}$$

It follows that $h = k = e$. (Why?) Thus, ϕ is one-to-one. (Why?)

(iv) onto: Trivial. (Why?)

□

Example 2

Let G be a finite abelian group. Let $n \in \mathbf{Z}^+$. Define a function

$$\phi : G \to G \text{ by } \phi(g) = g^n, \text{ for all } g \in G.$$

Then ϕ is a group isomorphism if and only if G has no nontrivial element whose order is a divisor of n.

Proof.

Example 2

Let G be a finite abelian group. Let $n \in \mathbf{Z}^+$. Define a function

$$\phi : G \to G \text{ by } \phi(g) = g^n, \text{ for all } g \in G.$$

Then ϕ is a group isomorphism if and only if G has no nontrivial element whose order is a divisor of n.

Proof.

(i) well-defined:

Example 2

Let G be a finite abelian group. Let $n \in \mathbf{Z}^+$. Define a function

$$\phi : G \to G \text{ by } \phi(g) = g^n, \text{ for all } g \in G.$$

Then ϕ is a group isomorphism if and only if G has no nontrivial element whose order is a divisor of n.

Proof.

(i) well-defined: Trivial. (Why?)

(ii) ϕ preserves the products:

Example 2

Let G be a finite abelian group. Let $n \in \mathbf{Z}^+$. Define a function

$$\phi : G \to G \text{ by } \phi(g) = g^n, \text{ for all } g \in G.$$

Then ϕ is a group isomorphism if and only if G has no nontrivial element whose order is a divisor of n.

Proof.

(i) well-defined: Trivial. (Why?)

(ii) ϕ preserves the products: For any $g, h \in G$, we have

$$\phi(gh) = (gh)^n \overset{!}{=} g^n h^n = \phi(g)\phi(h).$$

(iii) one-to-one and onto:

Example 2

Let G be a finite abelian group. Let $n \in \mathbf{Z}^+$. Define a function

$$\phi : G \to G \text{ by } \phi(g) = g^n, \text{ for all } g \in G.$$

Then ϕ is a group isomorphism if and only if G has no nontrivial element whose order is a divisor of n.

Proof.

(i) well-defined: Trivial. (Why?)

(ii) ϕ preserves the products: For any $g, h \in G$, we have

$$\phi(gh) = (gh)^n \overset{!}{=} g^n h^n = \phi(g)\phi(h).$$

(iii) one-to-one and onto: If ϕ is one-to-one, then ϕ is also onto. (Why?)

Example 2

Let G be a finite abelian group. Let $n \in \mathbf{Z}^+$. Define a function

$$\phi : G \to G \text{ by } \phi(g) = g^n, \text{ for all } g \in G.$$

Then ϕ is a group isomorphism if and only if G has no nontrivial element whose order is a divisor of n.

Proof.

(i) well-defined: Trivial. (Why?)

(ii) ϕ preserves the products: For any $g, h \in G$, we have

$$\phi(gh) = (gh)^n \overset{!}{=} g^n h^n = \phi(g)\phi(h).$$

(iii) one-to-one and onto: If ϕ is one-to-one, then ϕ is also onto. (Why?) By Proposition 5 in §3.4, ϕ is one-to-one $\Leftrightarrow$ $\phi(g) = e \Rightarrow g = e$.

$\Leftrightarrow$

Example 2

Let G be a finite abelian group. Let $n \in \mathbf{Z}^+$. Define a function

$$\phi : G \to G \text{ by } \phi(g) = g^n, \text{ for all } g \in G.$$

Then ϕ is a group isomorphism if and only if G has no nontrivial element whose order is a divisor of n.

Proof.

(i) well-defined: Trivial. (Why?)

(ii) ϕ preserves the products: For any $g, h \in G$, we have

$$\phi(gh) = (gh)^n \stackrel{!}{=} g^n h^n = \phi(g)\phi(h).$$

(iii) one-to-one and onto: If ϕ is one-to-one, then ϕ is also onto. (Why?)
By Proposition 5 in §3.4, ϕ is one-to-one $\Leftrightarrow \phi(g) = e \Rightarrow g = e$.

$$\Leftrightarrow g^n = e \Rightarrow g = e \Leftrightarrow$$

Example 2

Let G be a finite abelian group. Let $n \in \mathbf{Z}^+$. Define a function

$$\phi : G \to G \text{ by } \phi(g) = g^n, \text{ for all } g \in G.$$

Then ϕ is a group isomorphism if and only if G has no nontrivial element whose order is a divisor of n.

Proof.

(i) well-defined: Trivial. (Why?)

(ii) ϕ preserves the products: For any $g, h \in G$, we have

$$\phi(gh) = (gh)^n \stackrel{!}{=} g^n h^n = \phi(g)\phi(h).$$

(iii) one-to-one and onto: If ϕ is one-to-one, then ϕ is also onto. (Why?)
By Proposition 5 in §3.4, ϕ is one-to-one $\Leftrightarrow \phi(g) = e \Rightarrow g = e$.

$$\Leftrightarrow g^n = e \Rightarrow g = e \Leftrightarrow o(g) \nmid n \text{ for all } g \neq e.$$

Example 2

Let G be a finite abelian group. Let $n \in \mathbf{Z}^+$. Define a function

$$\phi : G \to G \text{ by } \phi(g) = g^n, \text{ for all } g \in G.$$

Then ϕ is a group isomorphism if and only if G has no nontrivial element whose order is a divisor of n.

Proof.

(i) well-defined: Trivial. (Why?)

(ii) ϕ preserves the products: For any $g, h \in G$, we have

$$\phi(gh) = (gh)^n \overset{!}{=} g^n h^n = \phi(g)\phi(h).$$

(iii) one-to-one and onto: If ϕ is one-to-one, then ϕ is also onto. (Why?)
By Proposition 5 in §3.4, ϕ is one-to-one $\Leftrightarrow$ $\phi(g) = e \Rightarrow g = e$.

$$\Leftrightarrow g^n = e \Rightarrow g = e \Leftrightarrow o(g) \nmid n \text{ for all } g \neq e.$$

That is, G has no non-identity element whose order is a divisor of n.

$\square$

Example 3

Any cyclic group of even order has exactly one element of order 2.

Proof.

Example 3

Any cyclic group of even order has exactly one element of order 2.

Proof.

Let G be a cyclic group of order $2n$. Thm 2 (b) in §3.5: $G \cong \mathbf{Z}_{2n}$.

Example 3

Any cyclic group of even order has exactly one element of order 2.

Proof.

Let G be a cyclic group of order $2n$. Thm 2 (b) in §3.5: $G \cong \mathbf{Z}_{2n}$. In $\mathbf{Z}_{2n}$, $o(x) = 2 \Rightarrow 2x \equiv 0 \pmod{2n} \Rightarrow x \equiv 0 \pmod{n} \Rightarrow x \equiv 0, n \pmod{2n}$, i.e., $x = [0]_{2n}, [n]_{2n}$.

Example 3

Any cyclic group of even order has exactly one element of order 2.

Proof.

Let G be a cyclic group of order $2n$. Thm 2 (b) in §3.5: $G \cong \mathbf{Z}_{2n}$. In $\mathbf{Z}_{2n}$, $o(x) = 2 \Rightarrow 2x \equiv 0 \pmod{2n} \Rightarrow x \equiv 0 \pmod{n} \Rightarrow x \equiv 0, n \pmod{2n}$, i.e., $x = [0]_{2n}, [n]_{2n}$. But $o([0]_{2n}) = 1$, $[n]_{2n}$ is the only element of order 2 in $\mathbf{Z}_{2n}$.

Example 3

Any cyclic group of even order has exactly one element of order 2.

Proof.

Let G be a cyclic group of order $2n$. Thm 2 (b) in §3.5: $G \cong \mathbf{Z}_{2n}$. In $\mathbf{Z}_{2n}$, $o(x) = 2 \Rightarrow 2x \equiv 0 \pmod{2n} \Rightarrow x \equiv 0 \pmod{n} \Rightarrow x \equiv 0, n \pmod{2n}$, i.e., $x = [0]_{2n}, [n]_{2n}$. But $o([0]_{2n}) = 1$, $[n]_{2n}$ is the only element of order 2 in $\mathbf{Z}_{2n}$. The proof is done. (Why?) [

Example 3

Any cyclic group of even order has exactly one element of order 2.

Proof.

Let G be a cyclic group of order $2n$. Thm 2 (b) in §3.5: $G \cong \mathbf{Z}_{2n}$. In $\mathbf{Z}_{2n}$, $o(x) = 2 \Rightarrow 2x \equiv 0 \pmod{2n} \Rightarrow x \equiv 0 \pmod{n} \Rightarrow x \equiv 0, n \pmod{2n}$, i.e., $x = [0]_{2n}, [n]_{2n}$. But $o([0]_{2n}) = 1$, $[n]_{2n}$ is the only element of order 2 in $\mathbf{Z}_{2n}$. The proof is done. (Why?) [Proposition 3 (a) in §3.4] $\square$

Another proof.

Example 3

Any cyclic group of even order has exactly one element of order 2.

Proof.

Let G be a cyclic group of order $2n$. Thm 2 (b) in §3.5: $G \cong \mathbf{Z}_{2n}$. In $\mathbf{Z}_{2n}$, $o(x) = 2 \Rightarrow 2x \equiv 0 \pmod{2n} \Rightarrow x \equiv 0 \pmod{n} \Rightarrow x \equiv 0, n \pmod{2n}$, i.e., $x = [0]_{2n}, [n]_{2n}$. But $o([0]_{2n}) = 1$, $[n]_{2n}$ is the only element of order 2 in $\mathbf{Z}_{2n}$. The proof is done. (Why?) [Proposition 3 (a) in §3.4] $\square$

Another proof.

$G \cong \mathbf{Z}_{2n}$:

Example 3

Any cyclic group of even order has exactly one element of order 2.

Proof.

Let G be a cyclic group of order $2n$. Thm 2 (b) in §3.5: $G \cong \mathbf{Z}_{2n}$. In $\mathbf{Z}_{2n}$, $o(x) = 2 \Rightarrow 2x \equiv 0 \pmod{2n} \Rightarrow x \equiv 0 \pmod{n} \Rightarrow x \equiv 0, n \pmod{2n}$, i.e., $x = [0]_{2n}, [n]_{2n}$. But $o([0]_{2n}) = 1$, $[n]_{2n}$ is the only element of order 2 in $\mathbf{Z}_{2n}$. The proof is done. (Why?) [Proposition 3 (a) in §3.4] □

Another proof.

$G \cong \mathbf{Z}_{2n}$: In $\mathbf{Z}_{2n}$, there is exactly one subgroup H of order 2. (Why?)

Example 3

Any cyclic group of even order has exactly one element of order 2.

Proof.

Let G be a cyclic group of order $2n$. Thm 2 (b) in §3.5: $G \cong \mathbf{Z}_{2n}$. In $\mathbf{Z}_{2n}$, $o(x) = 2 \Rightarrow 2x \equiv 0 \pmod{2n} \Rightarrow x \equiv 0 \pmod{n} \Rightarrow x \equiv 0, n \pmod{2n}$, i.e., $x = [0]_{2n}, [n]_{2n}$. But $o([0]_{2n}) = 1$, $[n]_{2n}$ is the only element of order 2 in $\mathbf{Z}_{2n}$. The proof is done. (Why?) [Proposition 3 (a) in §3.4] $\square$

Another proof.

$G \cong \mathbf{Z}_{2n}$: In $\mathbf{Z}_{2n}$, there is exactly one subgroup H of order 2. (Why?) Moreover, H is cyclic. (Why?)

Example 3

Any cyclic group of even order has exactly one element of order 2.

Proof.

Let G be a cyclic group of order $2n$. Thm 2 (b) in §3.5: $G \cong \mathbf{Z}_{2n}$. In $\mathbf{Z}_{2n}$, $o(x) = 2 \Rightarrow 2x \equiv 0 \pmod{2n} \Rightarrow x \equiv 0 \pmod{n} \Rightarrow x \equiv 0, n \pmod{2n}$, i.e., $x = [0]_{2n}, [n]_{2n}$. But $o([0]_{2n}) = 1$, $[n]_{2n}$ is the only element of order 2 in $\mathbf{Z}_{2n}$. The proof is done. (Why?) [Proposition 3 (a) in §3.4] $\square$

Another proof.

$G \cong \mathbf{Z}_{2n}$: In $\mathbf{Z}_{2n}$, there is exactly one subgroup H of order 2. (Why?) Moreover, H is cyclic. (Why?) Thus, $H \cong \mathbf{Z}_2$. (Why?)

Example 3

Any cyclic group of even order has exactly one element of order 2.

Proof.

Let G be a cyclic group of order $2n$. Thm 2 (b) in §3.5: $G \cong \mathbf{Z}_{2n}$. In $\mathbf{Z}_{2n}$, $o(x) = 2 \Rightarrow 2x \equiv 0 \pmod{2n} \Rightarrow x \equiv 0 \pmod{n} \Rightarrow x \equiv 0, n \pmod{2n}$, i.e., $x = [0]_{2n}, [n]_{2n}$. But $o([0]_{2n}) = 1$, $[n]_{2n}$ is the only element of order 2 in $\mathbf{Z}_{2n}$. The proof is done. (Why?) [Proposition 3 (a) in §3.4] $\square$

Another proof.

$G \cong \mathbf{Z}_{2n}$: In $\mathbf{Z}_{2n}$, there is exactly one subgroup H of order 2. (Why?) Moreover, H is cyclic. (Why?) Thus, $H \cong \mathbf{Z}_2$. (Why?) It follows that H has only one generator. (Why?)

Example 3

Any cyclic group of even order has exactly one element of order 2.

Proof.

Let G be a cyclic group of order $2n$. Thm 2 (b) in §3.5: $G \cong \mathbf{Z}_{2n}$. In $\mathbf{Z}_{2n}$, $o(x) = 2 \Rightarrow 2x \equiv 0 \pmod{2n} \Rightarrow x \equiv 0 \pmod{n} \Rightarrow x \equiv 0, n \pmod{2n}$, i.e., $x = [0]_{2n}, [n]_{2n}$. But $o([0]_{2n}) = 1$, $[n]_{2n}$ is the only element of order 2 in $\mathbf{Z}_{2n}$. The proof is done. (Why?) [Proposition 3 (a) in §3.4] □

Another proof.

$G \cong \mathbf{Z}_{2n}$: In $\mathbf{Z}_{2n}$, there is exactly one subgroup H of order 2. (Why?) Moreover, H is cyclic. (Why?) Thus, $H \cong \mathbf{Z}_2$. (Why?) It follows that H has only one generator. (Why?) Similarly as above, the proof is done. □

Example 1

$\mathbf{Z}_{15}^{\times}$ is not cyclic:

Example 3

Any cyclic group of even order has exactly one element of order 2.

Proof.

Let G be a cyclic group of order $2n$. Thm 2 (b) in §3.5: $G \cong \mathbf{Z}_{2n}$. In $\mathbf{Z}_{2n}$, $o(x) = 2 \Rightarrow 2x \equiv 0 \pmod{2n} \Rightarrow x \equiv 0 \pmod{n} \Rightarrow x \equiv 0, n \pmod{2n}$, i.e., $x = [0]_{2n}, [n]_{2n}$. But $o([0]_{2n}) = 1$, $[n]_{2n}$ is the only element of order 2 in $\mathbf{Z}_{2n}$. The proof is done. (Why?) [Proposition 3 (a) in §3.4] □

Another proof.

$G \cong \mathbf{Z}_{2n}$: In $\mathbf{Z}_{2n}$, there is exactly one subgroup H of order 2. (Why?) Moreover, H is cyclic. (Why?) Thus, $H \cong \mathbf{Z}_2$. (Why?) It follows that H has only one generator. (Why?) Similarly as above, the proof is done. □

Example 1

$\mathbf{Z}_{15}^{\times}$ is not cyclic: $[-1]_{15}$ and $[4]_{15}$ have order 2. (Much easier!)
$\mathbf{Z}_{21}^{\times}$ is not cyclic:

Example 3

Any cyclic group of even order has exactly one element of order 2.

Proof.

Let G be a cyclic group of order $2n$. Thm 2 (b) in §3.5: $G \cong \mathbf{Z}_{2n}$. In $\mathbf{Z}_{2n}$, $o(x) = 2 \Rightarrow 2x \equiv 0 \pmod{2n} \Rightarrow x \equiv 0 \pmod{n} \Rightarrow x \equiv 0, n \pmod{2n}$, i.e., $x = [0]_{2n}, [n]_{2n}$. But $o([0]_{2n}) = 1$, $[n]_{2n}$ is the only element of order 2 in $\mathbf{Z}_{2n}$. The proof is done. (Why?) [Proposition 3 (a) in §3.4] □

Another proof.

$G \cong \mathbf{Z}_{2n}$: In $\mathbf{Z}_{2n}$, there is exactly one subgroup H of order 2. (Why?) Moreover, H is cyclic. (Why?) Thus, $H \cong \mathbf{Z}_2$. (Why?) It follows that H has only one generator. (Why?) Similarly as above, the proof is done. □

Example 1

$\mathbf{Z}_{15}^{\times}$ is not cyclic: $[-1]_{15}$ and $[4]_{15}$ have order 2. (Much easier!)
$\mathbf{Z}_{21}^{\times}$ is not cyclic: $[-1]_{21}$ and $[8]_{21}$ have order 2. (Much easier!)

Example 4

Remark 1 (From previous example:)

In $\mathbf{Z}_{2n}$*, the equation* $2x \equiv 0 \pmod{2n}$ *has exactly* 2 *solutions.*
That is, the equation $x^2 = e$ *has exactly* 2 *solutions in* $G \cong \mathbf{Z}_{2n}$.

Example 4

Remark 1 (From previous example:)

In $\mathbf{Z}_{2n}$, the equation $2x \equiv 0 \pmod{2n}$ has exactly 2 solutions.
That is, the equation $x^2 = e$ has exactly 2 solutions in $G \cong \mathbf{Z}_{2n}$.

Let G be a finite cyclic group of order n. Let $m \in \mathbf{Z}^+$ be a divisor of n. Show that the equation $x^m = e$ has exactly m solutions.

Proof.

Example 4

Remark 1 (From previous example:)

In $\mathbf{Z}_{2n}$, the equation $2x \equiv 0 \pmod{2n}$ has exactly 2 solutions.
That is, the equation $x^2 = e$ has exactly 2 solutions in $G \cong \mathbf{Z}_{2n}$.

Let G be a finite cyclic group of order n. Let $m \in \mathbf{Z}^+$ be a divisor of n. Show that the equation $x^m = e$ has exactly m solutions.

Proof.

$G \cong \mathbf{Z}_n$: *To show* $mx \equiv 0 \pmod{n}$ has exactly m solutions, where $m|n$.

Example 4

Remark 1 (From previous example:)

In $\mathbf{Z}_{2n}$, the equation $2x \equiv 0 \pmod{2n}$ has exactly 2 solutions.
That is, the equation $x^2 = e$ has exactly 2 solutions in $G \cong \mathbf{Z}_{2n}$.

Let G be a finite cyclic group of order n. Let $m \in \mathbf{Z}^+$ be a divisor of n. Show that the equation $x^m = e$ has exactly m solutions.

Proof.

$G \cong \mathbf{Z}_n$: *To show* $mx \equiv 0 \pmod{n}$ has exactly m solutions, where $m | n$.
Then the proof is done by using Theorem 10 (2) in Chapter 1. (Why?) □

Theorem 2 (Theorem 10 in Chapter 1)

Example 4

Remark 1 (From previous example:)

In $\mathbf{Z}_{2n}$, the equation $2x \equiv 0 \pmod{2n}$ has exactly 2 solutions.
That is, the equation $x^2 = e$ has exactly 2 solutions in $G \cong \mathbf{Z}_{2n}$.

Let G be a finite cyclic group of order n. Let $m \in \mathbf{Z}^+$ be a divisor of n. Show that the equation $x^m = e$ has exactly m solutions.

Proof.

$G \cong \mathbf{Z}_n$: *To show* $mx \equiv 0 \pmod{n}$ has exactly m solutions, where $m|n$. Then the proof is done by using Theorem 10 (2) in Chapter 1. (Why?) □

Theorem 2 (Theorem 10 in Chapter 1)

Let a, b and $n > 1$ be integers.

(1) *The congruence $ax \equiv b \pmod{n}$ has a solution if and only if b is divisible by d, where $d = (a, n)$.*

(2) *If $d|b$, then there are d distinct solutions modulo n, and these solutions are congruent modulo n/d.*

Example 5

Let $H = \left\{ \begin{bmatrix} 1 & 0 \\ c & d \end{bmatrix} \;\middle|\; c \in \mathbf{Z}_p \text{ and } d = \pm 1 \right\} \subseteq \mathrm{GL}_2(\mathbf{Z}_p)$. Prove $H \cong D_p$.

Proof.

Example 5

Let $H = \left\{ \begin{bmatrix} 1 & 0 \\ c & d \end{bmatrix} \,\middle|\, c \in \mathbf{Z}_p \text{ and } d = \pm 1 \right\} \subseteq \mathrm{GL}_2(\mathbf{Z}_p)$. Prove $H \cong D_p$.

Proof.

H is a subgroup of $\mathrm{GL}_2(\mathbf{Z}_p)$. (Check it!)

Example 5

Let $H = \left\{ \begin{bmatrix} 1 & 0 \\ c & d \end{bmatrix} \,\middle|\, c \in \mathbf{Z}_p \text{ and } d = \pm 1 \right\} \subseteq \mathrm{GL}_2(\mathbf{Z}_p)$. Prove $H \cong D_p$.

Proof.

H is a subgroup of $\mathrm{GL}_2(\mathbf{Z}_p)$. (Check it!) And $|H| = 2p = |D_p|$.
$D_p =$

Example 5

Let $H = \left\{ \begin{bmatrix} 1 & 0 \\ c & d \end{bmatrix} \;\middle|\; c \in \mathbf{Z}_p \text{ and } d = \pm 1 \right\} \subseteq \mathrm{GL}_2(\mathbf{Z}_p)$. Prove $H \cong D_p$.

Proof.

H is a subgroup of $\mathrm{GL}_2(\mathbf{Z}_p)$. (Check it!) And $|H| = 2p = |D_p|$.
$D_p = \{a^k, a^k b \mid 0 \leq k < p\}$, where $a^p = e$, $b^2 = e$, $ba = a^{-1}b$.

Example 5

Let $H = \left\{ \begin{bmatrix} 1 & 0 \\ c & d \end{bmatrix} \;\middle|\; c \in \mathbf{Z}_p \text{ and } d = \pm 1 \right\} \subseteq \mathrm{GL}_2(\mathbf{Z}_p)$. Prove $H \cong D_p$.

Proof.

H is a subgroup of $\mathrm{GL}_2(\mathbf{Z}_p)$. (Check it!) And $|H| = 2p = |D_p|$.
$D_p = \{a^k, a^k b \mid 0 \leq k < p\}$, where $a^p = e$, $b^2 = e$, $ba = a^{-1}b$. Let

$$A = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \quad \text{and} \quad B = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$

Example 5

Let $H = \left\{ \begin{bmatrix} 1 & 0 \\ c & d \end{bmatrix} \,\middle|\, c \in \mathbf{Z}_p \text{ and } d = \pm 1 \right\} \subseteq \mathrm{GL}_2(\mathbf{Z}_p)$. Prove $H \cong D_p$.

Proof.

H is a subgroup of $\mathrm{GL}_2(\mathbf{Z}_p)$. (Check it!) And $|H| = 2p = |D_p|$.
$D_p = \{a^k, a^k b \mid 0 \leq k < p\}$, where $a^p = e$, $b^2 = e$, $ba = a^{-1}b$. Let

$$A = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \quad \text{and} \quad B = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$

Then $A^p = I_2$, $B^2 = I_2$

Example 5

Let $H = \left\{ \begin{bmatrix} 1 & 0 \\ c & d \end{bmatrix} \;\middle|\; c \in \mathbf{Z}_p \text{ and } d = \pm 1 \right\} \subseteq \mathrm{GL}_2(\mathbf{Z}_p)$. Prove $H \cong D_p$.

Proof.

H is a subgroup of $\mathrm{GL}_2(\mathbf{Z}_p)$. (Check it!) And $|H| = 2p = |D_p|$.
$D_p = \{a^k, a^k b \mid 0 \leq k < p\}$, where $a^p = e$, $b^2 = e$, $ba = a^{-1}b$. Let

$$A = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \quad \text{and} \quad B = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$

Then $A^p = I_2$, $B^2 = I_2$ and $A^k \neq A^k B$ for $0 \leq k < p$. (Check it!)

Example 5

Let $H = \left\{ \begin{bmatrix} 1 & 0 \\ c & d \end{bmatrix} \;\middle|\; c \in \mathbf{Z}_p \text{ and } d = \pm 1 \right\} \subseteq \mathrm{GL}_2(\mathbf{Z}_p)$. Prove $H \cong D_p$.

Proof.

H is a subgroup of $\mathrm{GL}_2(\mathbf{Z}_p)$. (Check it!) And $|H| = 2p = |D_p|$.
$D_p = \{a^k, a^k b \mid 0 \leq k < p\}$, where $a^p = e$, $b^2 = e$, $ba = a^{-1}b$. Let

$$A = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \quad \text{and} \quad B = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$

Then $A^p = I_2$, $B^2 = I_2$ and $A^k \neq A^k B$ for $0 \leq k < p$. (Check it!) Moreover,

$$BA = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ -1 & -1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ -1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} = A^{-1}B.$$

Example 5

Let $H = \left\{ \begin{bmatrix} 1 & 0 \\ c & d \end{bmatrix} \,\middle|\, c \in \mathbf{Z}_p \text{ and } d = \pm 1 \right\} \subseteq \mathrm{GL}_2(\mathbf{Z}_p)$. Prove $H \cong D_p$.

Proof.

H is a subgroup of $\mathrm{GL}_2(\mathbf{Z}_p)$. (Check it!) And $|H| = 2p = |D_p|$.
$D_p = \{a^k, a^k b \mid 0 \le k < p\}$, where $a^p = e$, $b^2 = e$, $ba = a^{-1}b$. Let

$$A = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \quad \text{and} \quad B = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$

Then $A^p = I_2$, $B^2 = I_2$ and $A^k \neq A^k B$ for $0 \le k < p$. (Check it!) Moreover,

$$BA = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ -1 & -1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ -1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} = A^{-1}B.$$

Thus, we can define $\phi : H \to D_p$ by $\phi(A) = a$ and $\phi(B) = b$.

Example 5

Let $H = \left\{ \begin{bmatrix} 1 & 0 \\ c & d \end{bmatrix} \;\middle|\; c \in \mathbf{Z}_p \text{ and } d = \pm 1 \right\} \subseteq \mathrm{GL}_2(\mathbf{Z}_p)$. Prove $H \cong D_p$.

Proof.

H is a subgroup of $\mathrm{GL}_2(\mathbf{Z}_p)$. (Check it!) And $|H| = 2p = |D_p|$.
$D_p = \{a^k, a^k b \mid 0 \le k < p\}$, where $a^p = e$, $b^2 = e$, $ba = a^{-1}b$. Let

$$A = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \quad \text{and} \quad B = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$

Then $A^p = I_2$, $B^2 = I_2$ and $A^k \neq A^k B$ for $0 \le k < p$. (Check it!) Moreover,

$$BA = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ -1 & -1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ -1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} = A^{-1}B.$$

Thus, we can define $\phi : H \to D_p$ by $\phi(A) = a$ and $\phi(B) = b$.
From the above calculations, it is clear that ϕ is a group isomorphism. $\square$

Example 6: Prove that $A_4 \ncong S_3 \times \mathbf{Z}_2$.

Note 1 (Proposition 6 in §3.6)

Example 6: Prove that $A_4 \not\cong S_3 \times \mathbf{Z}_2$.

Note 1 (Proposition 6 in §3.6)

A_4 has no subgroup of order 6.

Question 1

Example 6: Prove that $A_4 \not\cong S_3 \times \mathbf{Z}_2$.

Note 1 (Proposition 6 in §3.6)

A_4 has no subgroup of order 6.

Question 1

Does $S_3 \times \mathbf{Z}_2$ have a subgroup of order 6?

Example 6: Prove that $A_4 \not\cong S_3 \times \mathbf{Z}_2$.

Note 1 (Proposition 6 in §3.6)

A_4 has no subgroup of order 6.

Question 1

Does $S_3 \times \mathbf{Z}_2$ have a subgroup of order 6? *Yes!*

Claim 1

Example 6: Prove that $A_4 \not\cong S_3 \times \mathbf{Z}_2$.

Note 1 (Proposition 6 in §3.6)

A_4 has no subgroup of order 6.

Question 1

Does $S_3 \times \mathbf{Z}_2$ have a subgroup of order 6? *Yes!*

Claim 1

$S_3 \times \{[0]_2\}$ is a subgroup of $S_3 \times \mathbf{Z}_2$ of order 6. (Check it!)

Example 6: Prove that $A_4 \not\cong S_3 \times \mathbf{Z}_2$.

Note 1 (Proposition 6 in §3.6)

A_4 has no subgroup of order 6.

Question 1

Does $S_3 \times \mathbf{Z}_2$ have a subgroup of order 6? Yes!

Claim 1

$S_3 \times \{[0]_2\}$ is a subgroup of $S_3 \times \mathbf{Z}_2$ of order 6. (Check it!)
In particular, this is just a concrete example of Homework 4 (8) part (a).

Example 6: Prove that $A_4 \ncong S_3 \times \mathbf{Z}_2$.

Note 1 (Proposition 6 in §3.6)

A_4 has no subgroup of order 6.

Question 1

Does $S_3 \times \mathbf{Z}_2$ have a subgroup of order 6? *Yes!*

Claim 1

$S_3 \times \{[0]_2\}$ is a subgroup of $S_3 \times \mathbf{Z}_2$ of order 6. (Check it!)
In particular, this is just a concrete example of Homework 4 (8) part (a).

Thus, $A_4 \ncong S_3 \times \mathbf{Z}_2$.

Example 7: Prove that $S_4 \ncong A_4 \times \mathbf{Z}_2$.

Claim 2

Example 7: Prove that $S_4 \ncong A_4 \times \mathbf{Z}_2$.

Claim 2

The largest possible order of an element in S_4 is 4. (Why?)

Example 7: Prove that $S_4 \ncong A_4 \times \mathbf{Z}_2$.

Claim 2

The largest possible order of an element in S_4 is 4. (Why?)

Possible decomposition types of permutations of S_4: (See §3.6)

(i) a single cycle of length $1, 2, 3$ or 4

(ii) two disjoint cycles of length 2

Example 7: Prove that $S_4 \ncong A_4 \times \mathbf{Z}_2$.

Claim 2

The largest possible order of an element in S_4 is 4. (Why?)

Possible decomposition types of permutations of S_4: (See §3.6)

(i) a single cycle of length $1, 2, 3$ or 4

(ii) two disjoint cycles of length 2

And so the possible decomposition types of permutations of A_4 are

(a) a single cycle of length 1 or 3

(b) two disjoint cycles of length 2

Example 7: Prove that $S_4 \ncong A_4 \times \mathbf{Z}_2$.

Claim 2

The largest possible order of an element in S_4 is 4. (Why?)

Possible decomposition types of permutations of S_4: (See §3.6)

(i) a single cycle of length $1, 2, 3$ or 4

(ii) two disjoint cycles of length 2

And so the possible decomposition types of permutations of A_4 are

(a) a single cycle of length 1 or 3

(b) two disjoint cycles of length 2

It follows that there is an element of order 6 in $A_4 \times \mathbf{Z}_2$. (Why?)

Example 7: Prove that $S_4 \ncong A_4 \times \mathbf{Z}_2$.

Claim 2

The largest possible order of an element in S_4 is 4. (Why?)

Possible decomposition types of permutations of S_4: (See §3.6)

(i) a single cycle of length $1, 2, 3$ or 4

(ii) two disjoint cycles of length 2

And so the possible decomposition types of permutations of A_4 are

(a) a single cycle of length 1 or 3

(b) two disjoint cycles of length 2

It follows that there is an element of order 6 in $A_4 \times \mathbf{Z}_2$. (Why?)

Thus, $S_4 \ncong A_4 \times \mathbf{Z}_2$.